DELTA TECH AFRICA LIMITED

ISO/IEC 27017: 2015

IT SECURITY CONTROL

SUMMARY

ISO/IEC 27017:2015

The major concerns are that data might find up in the wrong hands, and what control a consumer has over irresponsible operators. But there are other worries as well: client identity, asset segregation on virtual servers, and what happens to assets if a CSP goes out of business are all problems for potential cloud customers. The ISO 27001 series tackles some of these issues, but a new standard, ISO/IEC 27017 Information technology — Security approaches, goes a step further and provides further assurance to potential cloud clients.

Cloud standards are technological standards that address cloud provider rules and guidelines directed at cloud service providers. ISO/IEC 27017 is unusual and particularly useful in that it gives information and assistance to both the CSP and the cloud service client. In addition to assuring the safety of services, ISO/IEC 27017 attempts to educate consumers on what they should expect from their cloud host.

The standard includes seven additional controls as well as cloud-based guidance on 37 of the controls in ISO/IEC 27002.

- **CLD.6.3.1:** The client and supplier must agree on shared or split responsibilities for information security duties connected with cloud services, which must be clearly spelled out, recorded, and communicated.
- **CLD.8.1.5:** Addresses how assets are returned or withdrawn from the cloud when the customer/provider contract/agreement is canceled.
- **CLD.9.5.1:** The provider is responsible for protecting and isolating the customer's virtual environment from other customers and other parties.
- **CLD.9.5.2:** The client and provider must guarantee that virtual machines are configured and hardened to satisfy the organization's requirements.
- **CLD.12.1.5:** It is the customer's obligation to establish, record, and monitor the administrative operations and processes connected with the cloud environment, and it is the CSP's responsibility to distribute documentation concerning important operations and procedures as needed by customers.
- **CLD.12.4.5:** How the provider's abilities allow the client to oversee activities in a cloud computing environment.
- **CLD.13.1.4:** Consistent configurations should be established to ensure that the network virtualization environment adheres to the physical network's information security policy.

Functions And Duties

Ambiguity in duties, as well as in the definition and allocation of responsibilities for problems such as data ownership, remote access, and infrastructure repair, can lead to commercial or legal challenges, particularly when working with third parties. As stated in the standard:

"Data and files produced or updated on the cloud service provider's systems during the usage of the cloud service might be crucial to the service's secure operation, recovery, and continuity." All assets should be specified and recorded, as should the parties responsible for actions related to these assets, such as backup and recovery procedures. Otherwise, there is a danger that the cloud service provider may expect that the cloud service customer would undertake these critical duties (or vice versa), resulting in data loss."

Essentially, the guideline mandates that it be obvious from the start who is responsible for what.

Controls For Security

It's not only the separation of responsibilities that the standard helps define: ISO/IEC 27017 also goes into much more detail about the type of security controls that service providers should be implementing helping reduce the barriers to cloud adoption.

ISO/IEC 27017 provides a method for cloud service providers to identify the number of controls in place. This implies that written proof, supported by independent sources such as certification to specific standards, demonstrates that relevant policies have been adopted and, more crucially, what sorts of controls have been established.

This information should be communicated with the cloud customer prior to signing any contract to assist relieve any prospective concerns. In cases where independent audits aren't practical or would pose a greater risk to information security, the standard does provide an option for CSPs to self-assess. When this is the case, the CSP must tell customers that they have self-assessed.

Cryptography

There is also advice on any encryption that is utilized. This is true for both the consumer and the supplier, as they both have obligations in this area. The company should explain how it uses cryptography and assist clients in implementing their own security measures. It should also address unique circumstances, such as health data, where additional regulatory rules may be required.

Customers should also be open about the sort of encryption they use – and they should use cryptography if the risk analysis indicates that it is necessary. In reality, it is this type of disagreement that drives the need for the standard. Not only should both parties be able to ensure each other that the network is secure, but they should also be able to guarantee each other that the two systems are compatible. Furthermore, it should be decided if these constraints apply to data at rest, in transit, or both, as this has previously created misconceptions.

Customer Interactions

The standard goes beyond technical requirements and includes training standards. Many clients are pleased with the architecture of cloud service providers but are concerned about the degree of assistance.

After all, there is plenty of data to demonstrate that workers are frequently the weakest link in any organization's security systems. Customers should be careful not simply of defective security gadgets, but also of whether employees are taking all necessary precautions. The new standard requires providers to not only provide training and awareness for workers and contractors, but also to address regulatory obligations, client access, and specific demands.

Asset Ownership

It might be difficult to determine who owns something in the cloud. The standard recommends creating an inventory of assets kept in the cloud and goes back to the ISO/IEC 27002 guiding information on asset ownership, permitted use, and return. The new standard specifies requirements for the secure disposal of client assets, ensuring that private data is not simply discarded in virtual bins.

Who Stands To Gain?

The short answer is "everyone." Everyone who is related with the cloud.

The path to the cloud might be fraught with misunderstandings and anxiety. Any firm that has entrusted customers' personal data to a third party has discovered that there are grey areas in which rights and duties are not clearly defined. A lot has been based on trust, which isn't always the best prescription for success.

CIOs and IT managers will be heartened by the changes in their interactions with CSPs enabled by the standard, which will provide a genuine level of confidence to cloud computing security. Orientation and implementation training centered on ISO/IEC 27017 may be highly beneficial when a business decides whether to utilize the cloud and which partners are most suited to their needs.

CSPs who opt to implement ISO/IEC 27017 will also benefit from knowing they are providing a safe solution that their clients can rely on, which goes a long way toward establishing a cloud-based partnership. And, of course, by collaborating with their customers during the adoption process, ISO/IEC 27017 safeguards them against potentially damaging claims or lawsuits that might disrupt their operation and tarnish their reputation.

ISO/IEC 27017 Protects Data In The Cloud

Analysts and industry professionals believe that cloud services' scalability and flexibility will continue to boost adoption. However, businesses ranging from large global web-based corporations to tiny firms and start-ups are still hesitant due to security concerns. ISO/IEC 27017 provides additional security controls for the cloud that ISO 27002 does not fully cover, as well as extra controls especially connected to cloud services, whether you are a cloud service provider or your business is considering hiring one. The standard's goal is to offer cloud service-specific controls, implementation instructions, and other data to assist minimize the risks associated with cloud services' technical and operational aspects. It guarantees that both cloud service users and cloud service providers understand who is accountable for what.

Benefits

- **Builds trust in your company** - by assuring consumers and stakeholders that their data and information is secure.
- **Competitive edge** - proves that strong data protection policies are in place.
- **Protects your brand** - minimizes the danger of negative publicity as a result of data breaches.
- **Reduces risks** - ensuring that hazards are identified and that mechanisms to manage or mitigate them are in place.
- **Prevents sanctions** - guarantees that local requirements are followed, lowering the possibility of fines for data breaches.
- **Assists in company growth** - by providing standard guidelines across countries, making it easier to do business abroad and acquire access as a favored supplier.

Facts

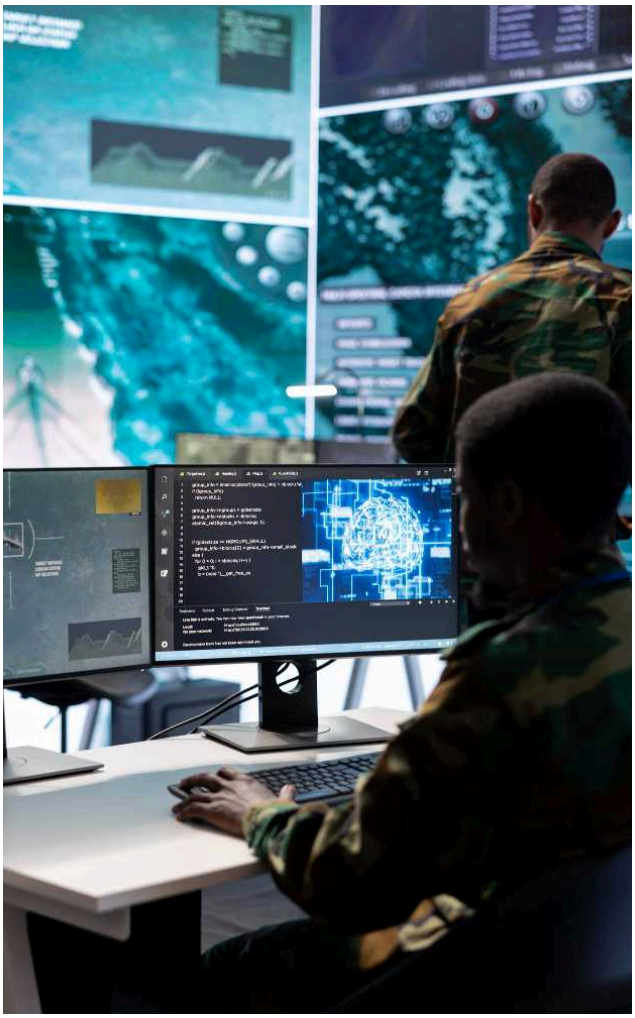
Cybercrime steals between 15% and 20% of the value produced through the Internet.
McAfee, 2014, Net Losses: Determining the Global Cost of Cybercrime

The main barrier to cloud initiatives, according to 73% of IT experts, is data security.
Cloud Security Alliance, Cloud Adoption Practices and Objectives Survey Report, 2015.

Sixty-one percent of IT professionals say that the security of data stored in the cloud is a top executive issue.
Cloud Security Alliance, Cloud Adoption Practices and Priorities Survey Report, 2015.

About DTA

Delta Tech Africa Limited Is An ICT And Quality Consulting Organization Focused On Performance Management Across Business Verticals. Delta Means“ A Finite Increment”. We Help Organizations To Achieve This Increment Across Departments And Functions And To Improve The Overall Organizational Performance While Adding Value To The Stakeholders. Evolution Is A Constant Change. When The Pace Of Evolution Renders Societies Impatient, It Is A Technology That Accelerates Evolution Leading To The Transformation Of Societies. When That Evolution Happens, It Doesn’t Limit The Human Endeavors, To Get The Technology Evolution, It Has To Be Supported By Processes And Management Of The Best Quality. Hence, We At Delta Tech Africa Thought Of Bringing Both Technology And Quality Management Processes Together To Get The Best Organizational Performance And Value Across The Fast Growing Continent Of Africa.



Our Offices

Nigeria | PLOT 55B, Baderinwa Alabi Street, Central Lekki Residents' Association , Rahman Adeboyejo Street Lekki Phase 1, Lagos, Nigeria
Kenya | P.O.Box 39562-00623, Parklands, Nairobi, Kenya.
Ghana | Plot 3, Dade Link, Off Dade Street, Labone, Accra, Ghana.
South Africa | 1 Waterhouse Place Century City Cape Town 7441

Our Phone Numbers

+27 63 933 1982, +27 10 594 5356

Our Email

info@dtafrica.com

Our Website

https://www.dtafrica.com

DELTA TECH AFRICA LIMITED

info@dtafrica.com | www.dtafrica.com

© 2024 Delta Tech Africa. All Rights Reserved